

SEALED

IN THE
UNITED STATES DISTRICT COURT
FOR THE
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
UNIQUE FACEBOOK IDENTIFICATION
NUMBERS AND ASSOCIATED ALIASES,
IDENTIFIED IN ATTACHMENT A THAT
ARE STORED AT PREMISES
CONTROLLED BY FACEBOOK

Case No.

3:13-mj-00051

Filed Under Seal

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Rebecca Gonzalez-Ramos, a Special Agent with Homeland Security Investigations (HSI), having been first duly sworn, hereby depose and state the following:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook accounts that is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered at 151 University Avenue, Palo Alto, California, 94301. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the web sites.

2. I am a Special Agent with U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) currently assigned to the Cyber Crimes Center (C3), Child Exploitation Investigations Unit. I have been a sworn law enforcement officer since 2002. I am responsible for conducting federal and international investigations relating to crimes involving

YCB
10/10/2013

the sexual exploitation of children. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and have received basic, advanced, and on-the-job training in the investigation of cases involving the sexual exploitation of children. I have investigated Child Exploitation cases for a period of seven years and supervised the Child Exploitation Group for a period of five years. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251(a) and (e) (production and attempted production of child pornography), Title 18, United States Code Section 2422(b) (enticement and attempted enticement of a minor), Title 18, United States Code, Sections 2252A(a)(1) and (2) and (b) (transportation and distribution, and attempted transportation and distribution, of child pornography), and Title 18, United States Code, Section 875(d) (extortion), have been committed by an individual using the multiple Facebook accounts included in Attachment A. There is also probable cause to search the information described in Attachment B for evidence of these crimes.

Applicable Statutes

5. Title 18, United States Code, §§ 2251(a) and (e) prohibits a person from employing, using, or enticing a minor to engage in sexually explicit conduct for the purpose of producing a

[Handwritten signature]
12/10/2013

visual depiction of that conduct, or attempting to do so. Title 18, United States Code, § 2256(2)(A) provides that sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, bestiality, masturbation, sadistic or masochistic abuse, or the lascivious exhibition of the genitals or pubic area of any person.

6. Title 18, United States Code, § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempting to do so.

7. Title 18, United States Code, § 2252A(a)(1) and (b) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer any child pornography, or attempting to do so; United States Code, § 2252A(a)(2) and (b) prohibits a person from knowingly receiving or distributing any child pornography, or any material that contains child pornography, that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means including by computer, or attempting to do so.

8. Title 18, United States Code, § 875(d) prohibits any person from transmitting in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, with intent to extort from any person, firm, association, or corporation, any money or other thing of value.

Definitions

9. The following definitions apply to this Affidavit and its Attachments:

a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

- i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

10/10/2013

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

k. “Browser cookie” is a small file or part of a file stored on a World Wide Web user’s computer, created and subsequently read by a Web site server, and containing personal information such as a user identification code, customized preferences, or a record of pages visited.

Background Regarding Computers, the Internet, and Email

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornography formerly was produced

MS
10/11/2003

using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls.

b. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

c. Individuals can now transfer photographs from a camera onto a computer-readable format. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store over 100 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

d. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to

Handwritten: 10/10/2003

literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte (1000 gigabytes) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)

f. The Internet affords individuals several different venues for producing, obtaining, viewing, and distributing child pornography in a relatively secure and anonymous fashion.

g. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The

6863
10/10/2022

online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Technical Background on Facebook

11. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

12. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone

Handwritten:
10/10/2013

numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number (“UID”) to each account.

13. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

14. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “Mini-Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

15. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can

MS
10/10/2013

post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

16. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

17. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information.

Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. Private message are saved based on user discretion. If the user has deleted any messages at any point during their activity, Facebook does not keep records of those messages.

18. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

19. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

12/10/2013

20. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

21. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

22. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

23. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

24. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service

YJS
10/10/2013

(including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

Facts Supporting Probable Cause

26. In September 2013, the online social networking service Facebook contacted the Homeland Security Investigation's Cyber Crimes Center regarding an individual ("Target") that the Facebook Security Unit discovered, who was using Facebook as a platform to sexually entice and extort minor girls. The Facebook Security Unit conducted an internal investigation and discovered that the Target used several online platforms, including Facebook, to solicit nude videos and images of females, the vast majority of whom were minors, by threatening to share embarrassing pictures, including sexual images of the minors, with the minors' Facebook friends. According to the Facebook Security Unit, the Target also persuaded minors to appear naked, including at times to engage in sexually explicit conduct, during web camera chat sessions. The Target generally employs the same method of extortion with each minor female victim in that he first obtains a sexual photo or photos of the minor female victims, and then threatens to send these images to family and/or friends unless the minor female victims provide

1/8/13
10/10/2013

him with more images and/or webcam sessions showcasing sexual conduct. The Facebook Security Team identified at least thirty-three (33) minor female victims in the United States, who the Target had approached on Facebook in order to persuade them to create sexual images of themselves, including images depicting them engaging in sexually explicit conduct, and to send these images to him. The Facebook Security Unit's internal investigation did not reveal the identity of the Target. They were however able to determine that the Target was probably residing in The Netherlands.

27. The Facebook Security Unit identified ninety-six (96) Facebook UIDs belonging to the Target. The Facebook Security Unit was able to determine that these Facebook UIDs belonged to the same Target after conducting its internal investigation and determining that all these accounts were forensically linked. The Facebook Security Unit explained that "forensically linked" accounts were separate Facebook user accounts with distinct UIDs that were linked together by a common web browser on a common machine. The Facebook Security Unit was able to make this determination by identifying that the same browser cookie was being transmitted by each of these Facebook accounts.

28. Further, although there are ninety-six distinct UIDs, many of the names associated with those UIDs are either identical or similar. For example, one UID's associated name is "Mel Raine," while another UID's associated name is "Kelseeh Rayn." One UID's associated name is "Marc Cameronss" and another UID's associated name is "Marc Camerons." Moreover, Facebook has identified that the Target generally uses more than one identity to contact each minor female victim, and that he often uses the same identity to contact other minor female victims. For example, Facebook identified that UIDs associated with user names "Marc Cameronss," "Marc Camerons," and "Kelsey Bammerz" were used to contact one victim, and

Handwritten signature and date:
10/10/2013

then UUIDs associated with usernames “Marc Cameronss,” “Tyler Boo,” “Marc Camerons,” “Lars Merckin,” “Kyle Hymen Norito,” “Ashley Canter,” “Cody Cena,” and “Mel Raine” were used to contact a different victim. Each one of the ninety-six accounts have been identified by Facebook to be directly involved with the extortion of different female minors for the purpose of persuading these minor females to create sexual images of themselves, including images depicting them engaging in sexually explicit conduct. The Facebook UUIDs that the Facebook Security Unit identified as belonging to the Target are set forth in Attachment A.

29. According to the Facebook Security Unit, its internal investigation and analysis of the Target’s and victims’ accounts revealed that the Target employs the same method of extortion with all the minor female victims. The Target usually initiates the conversations with the victims posing as someone else. During the web camera chat sessions, the Target records the live footage and creates sexually explicit videos and images out of the recorded content. Then, the Target locates the Facebook profiles of the minors. The Target then documents the names and URLs of the minors’ friends and family members and then uses fake accounts on Facebook to contact the victims through “friend requests” and Facebook Messages. In many instances, the Target sends hyperlinks to images of the minors hosted on other websites to prove that he actually possesses footage of the victims. Then, the Target often reveals that he has a list of the victims’ friends and family members and threatens to send the content to people on the list if the victims refuse to follow his demands. Often the Target’s demands include a specified number of web camera chat sessions in which the victims must perform several sexual acts as instructed by the Target. If the victims fail to comply with his demands, or if they ignore his messages, the Target sends the content out to the victim’s friends and families. According to the Facebook Security Unit, the Target followed through on his threats on numerous occasions.

[Handwritten signature]
10/10/2013

30. The Facebook Security Unit identified Minor Female Victim 1 (“MFV 1”), in Charlottesville, VA, as one of the U.S. minor female victims contacted by the Target to engage in the extortionist activity previously detailed. According to the information provided by the Facebook Security Unit, the Target contacted MFV 1 on June 17, 2013 using two Facebook identities “Terliyam Hefter” and “Malinday Forsent” each with its own UID. According to the Facebook Security Unit, it was able to identify that these two accounts were forensically linked in that the transmission of the same browser cookie by both Facebook accounts indicated use on a common web browser on a common machine. The Facebook Security Unit conducted an internal review of the interaction between the Facebook accounts of MFV 1 and the Target, and reported that the Target had contacted MFV 1’s Facebook friends in his attempt to extort MFV 1 for sexual images. Their investigation further revealed that the Target had sent a link to MFV 1’s friends which ultimately led to an image depicting MFV 1 engaging in sexually explicit conduct. The Facebook Security Unit also noted the existence of photos of MFV 1 outside of Facebook posted by the Target.

31. The Facebook Security Unit’s internal investigation discovered the existence of a link to sexual images, related to MFV 1’s account, in the Target’s message inbox, which the Facebook Security Unit reported to the National Center for Missing and Exploited Children (“NCMEC”). NCMEC subsequently generated a report of this incident. Review of the NCMEC report of this incident revealed two sexual images of minors. One of the pictures depicts MFV 1 with her breasts exposed. The second image is a picture of another female naked with her legs open and her hand on her vagina. Facebook has identified this other female as a victim from the United Kingdom, who was also extorted by the Target’s “Terliyam Hefter” identity. Facebook identified a live link captured from the Target’s Facebook page which led to more sexually

20813
10/10/2013

explicit images of MFV 1. These include the picture of MFV 1's breast area previously described and another picture in the form of a collage that exhibits her breast area, and her pubic area. The collage depicts three distinct images of MFV 1. The first part of the collage depicts MFV 1 nude showing her face, but only depicts the right breast and abdomen region of MFV 1. The next part of the collage depicts MFV 1 completely nude and appears to be lying down. Both breasts are visible in the image. MFV 1 has her legs spread and slightly elevated and the central focus of this image is the display of her vaginal region. The last part of the collage is a close up of the vaginal region of MFV 1 and MFV 1 is manually manipulating her vaginal region with her right hand, her left breast is visible in the background of the picture. I conducted further investigation and discovered a website where MFV 1 identifies herself and indicates that she's a seventeen year old from Charlottesville, VA. I confirmed that this website containing information about this minor female in Charlottesville was indeed MFV 1 by confirming the email account MFV 1 provides in this website with an email account listed on a Facebook page named MFV1 Photography. Using the information initially provided by Facebook as well as the NCMEC report, I searched for and discovered MFV 1's Facebook page. I confirmed that the Facebook page I discovered was indeed of MFV 1. I also compared the image in the NCMEC report to the images found in MFV 1's Facebook page, and confirmed that I had found MFV 1's Facebook page. I reviewed MFV 1's Facebook page where she has display a senior manifesto, which led us to believe that she is actually on her 12th grade in school. The Facebook Security Unit also affirmatively identified MFV 1 to be a minor. An investigation of the link provided by the Facebook Investigation team which displays the sexually explicit images of MFV1 revealed an additional image of MFV1 with her family that is also displayed in MFV1 Facebook page.

MSB
10/10/2013

32. The Facebook Security Unit also identified Minor Female Victim 2 (“MFV 2”), in Homewood, IL, as another U.S. minor female victim contacted by the Target to engage in the extortionist activity previously detailed. Target contacted MFV 2 using a Facebook identity “Mel Raine.” According to the Facebook Security Unit, it was able to identify that “Mel Raine’s” Facebook account was forensically linked, using the methodology previously described, to the Target. The Facebook Security Unit conducted an internal review of the interaction between the Facebook accounts of MFV 2 and the Target, and reported that the Target had contacted MFV 2’s Facebook friends on June 29, 2013, presumably in his attempt to extort MFV 2 for sexual images. Their investigation further revealed that the Target had sent a link to MFV 2’s friends which presumably led to a sexual image of MFV 2.

33. The Facebook Security Unit’s internal investigation discovered the existence of a link leading to sexual images of MFV 1 and a different minor in the Target’s Facebook sent mailbox. These links were sent to MFV 2’s friends. The Facebook Security Unit reported these images to NCMEC and NCMEC subsequently generated a report of this incident. Review of the NCMEC report of this incident revealed four sexual images of what appears to be a minor. Three of the four pictures depict MFV 2 sitting with her legs spread open. Her breasts are clearly exposed as well as part of her vaginal area. Based on my years of experience investigating child exploitation offenses, she looks to be approximately 13 to 14 years old. Investigation revealed that MFV2 has a YouTube account that contains videos of her talking about different issues. In one of the videos, uploaded on October 8, 2012, MFV2 stated that she is 14 years old. The minor depicted in the video is the same minor depicted in the sexually explicit images referred to NCMEC by Facebook. The Facebook Security Unit also affirmatively identified MFV 2 to be a minor.

Handwritten signature and date:
12/10/2013

34. The Facebook Security Unit also identified Minor Female Victims 3 and 4 (MFV 3 and 4) from Lexington, Kentucky as additional U.S. minor female victims contacted by the Target to engage in the extortionist activity previously detailed. Target contacted both MFVs 3 and 4 using the Facebook identity "Tomas Coco Pops." Using the methodology previously described, the Facebook Security Unit was able to identify that "Tomas Coco Pops" Facebook account was forensically linked to the Target. The Facebook Security Unit conducted an internal review of the interaction between the Facebook accounts of MFVs 3 and 4 and the Target, and reported that the Target had contacted MFVs 3 and 4's Facebook friends on September 8, 2013. Their investigation further revealed that the Target had sent an image to MFV 3's and 4's family members.

35. According to the Facebook investigative report, another minor victim of the Target, was a fourteen year old minor female residing in British Columbia, Canada who committed suicide on October 10, 2012, after suffering from abusive bullying and being extorted in the manner described above. Facebook Security identified messages as far back as 2011 that indicate that this Canadian Minor was a target of the Target for an extended period of time. While it is unclear as to whether or not the Target was responsible for the initial nude images of the Canadian Minor that led to the initial blackmailing, the messages indicate that he sent out the content to many of her friends, family, and classmates. According to an investigative report created by the Facebook Security Unit, the Target monitored changes in the Canadian Minor's life for quite some time, including her moving and changing schools as a result of the humiliation and bullying that resulted from the content being sent to her peers. The Target used the changes to further commit threats, such as sending the content out to her new classmates once she changed schools. Facebook detected at least four conversations between the Target and

180
10/10/2013

the Canadian Minor which revealed that the Target was extorting the Canadian Minor to create sexually explicit images of herself and to engage in sex shows online for the Target. The chats between the Target and the Canadian Minor revealed that the Target threatened to send sexual images that he had of the Canadian Minor to her friends and family unless she engaged in online sex shows for him and/or create sexually explicit images of herself. According to the Facebook investigative report, on November 12, 2011 the Canadian Minor posted a status on her Facebook page that stated the following:

Posted 2011-11-12 19:29:53 UTC

Status: *I'm so sorry, everyone who got the links from austin collins. When I was 11 years old I got a message saying, 'I have all your information, I will come find you if you don't flash and do this for me' so I was scared, I said, 'one time okay' so I did it.. And he said if I didn't do it again he would send to all port coquitlam. I wasn't going to do it again, so then he sent it to everyone in port coquitlam. Teachers, friends family. On christmas. So I moved, I thought new start for my messup would be good, then he followed me.. He stalked and found out my new school and friends and now you guys all got the link. Judge me, or be there for me.. Wichever you guys want.. But right now I feel like shit, I feel so sad and sick.. That he's gonna do this for the rest of my life and there's nothing I can do. He made you all think he's a young boy in his teens that is going to westview when he's over 30+, he's tyler boo.. He's a sick pedofile. The best thing I can say now is, don't send it, block him, don't click it.. I really don't know what to do anymore.*

The Facebook investigative report also memorialized a chat between the Target and the Canadian Minor in October 2011, where the Target was attempting to extort additional sexual acts from the minor.

Tyler Boo: sup camwhore, been a while :P
i didnt send the video the last time because i liked how you whined , but as you know i have your new school, new schoolmates, new flash your parents have seen etc etc blahblah you know the drill.

so 3 shows of 15 minutes and then i wont send :3

Canadian Minor: Oh year what are some names ;)

WJB
10/10/2011

Tyler Boo: lol, u already forgot who i am? the guy who last year made you change school. got your door kicked in with cops in the morning :P

and also onyoutube like 6 months ago whatever, scared you a bit :P

you promised the authorities not to do be sexual on cam again because you are underage and it is considered producing child porn...well, you have. so i can send them that and make them come to you again, send your new school and friends and family again.

you will go through the exact same thing all over.

or you can give me 3 shows and i will disappear forever. You know I wont stop until you give me those 3 shows. if u go to a new school, new bf, new friends, new whatever, i will be there again :P

The Facebook Security Unit has forensically linked the UID associated with username "Tyler Boo," to the Target. The Facebook Security Unit indicated that they conducted a review of the Target's account and Canadian Minor's Facebook messages and were able to locate some of the nude pictures, screenshots, and video stills of the Canadian Minor that the Target sent to others through the Facebook Messages function, that were still available online as of October 2012. These indicate the various image-hosting services that the Target uses for uploading and sharing child exploitation content.

36. The true identity of the Target remains unknown at this time.

37. Based on my training, experience, and facts of this investigation, as well as on the methods used and representations of Facebook forensically linking the numerous accounts, UIDs and usernames to the Target, and based on my knowledge of how offenders maintain numerous parallel accounts on Facebook (each containing information relating to their actual identity), I believe evidence of a crime, evidence revealing the true identity of the Target, evidence of the pattern of criminal conduct employed by the Target, and information detailing the IP addresses utilized by the Target and therefore the location of the Target, is located in the accounts listed in

MSB
10/10/2013

Attachment A. It is therefore requested that this Court authorize the search of the full content of the accounts listed in Attachment A for identity and location evidence, as well as for fruits, instrumentalities and evidence of violations of the statutes cited herein.

Stored Wire and Electronic Communication Access

38. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled “Stored Wire and Electronic Communications and Transactional Records Access.”

39. Title 18, United States Code, Section 2703(a) states that the government may require a provider of electronic communication services to disclose the contents of electronic communications (less than 180 days old) by means of a federal or state search warrant.

40. Under Title 18, United States Code, Section 2703(b), the government may require a provider of remote computing services to disclose the contents of electronic communications (more than 180 days old) without notice to the subscriber or customer by means of a federal or state search warrant.

41. Under Title 18, United States Code, Section 2703(c), the government may require a provider of remote computing services or electronic communication services to disclose records and other information pertaining to their subscribers, or customers, by means of a federal or state search warrant. The government is not required to notify the subscriber/customer.

Information To Be Searched and Things to Be Seized

42. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

18A
10/10/2013

persons will review that information to locate the items described in Section II of Attachment B.

Conclusion

43. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Facebook there exists evidence of a crime, to wit: evidence of violations of Title 18, United States Code, Section 2251(a) and (e), that is Production and Attempted Production of Child Pornography, Title 18, United States Code Section 2422(b), Enticement and Attempted Enticement of a Minor, Title 18, United States Code Section, Title 18, United States Code, Sections 2252A(a)(1) and (2) and (b), Transportation and Distribution, and Attempted Transportation and Distribution, of Child Pornography, and Title 18, United States Code, Section 875(d), Extortion. Accordingly, a search warrant is requested.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Request to Seal, Order Non-Disclosure, & Keep Account Active

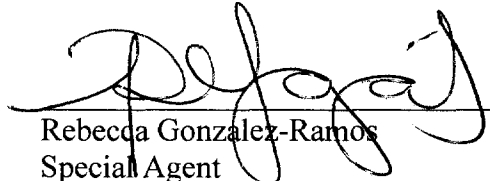
45. This is an ongoing investigation in which foreign law enforcement in conjunction with Child Exploitation Section at the HSI Cyber Crimes Center are working to identify the key perpetrators and to identify victims. Foreign law enforcement has provided, and continues to provide to U.S. law enforcement, investigative information pursuant to their undercover activity.

46. Because the Investigation is ongoing, your Affiant requests that this Application for Search Warrant, the Search Warrant, and supporting Affidavit in this matter be sealed until such time as the Court directs otherwise.

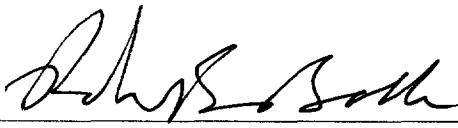
47. Pursuant to 18 U.S.C. § 2705(b), I would request the Court order Facebook, Inc. not to notify any other person of the existence of this warrant until further order of the Court. This

10/10/2013

request is made because I believe public knowledge of the warrant will seriously jeopardize the ongoing investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, notify confederates, or allow confederates to flee or continue flight from prosecution.


Rebecca Gonzalez-Ramos
Special Agent
Immigration & Customs Enforcement

Subscribed to and sworn before me this 10th day of October, 2013.


HONORABLE ROBERT S. BALLOU
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered at 151 University Avenue, Palo Alto, California, 94301 associated with the following Facebook account(s):

User IDs: 1616507556, 100000659608598, 100001572142810, 100001578424626, 100001580666568, 100001746389180, 100001747588302, 100001929381111, 100002353436107, 100002506557335, 100002544171178, 100002553207900, 100002735580148, 100002891689885, 100002910286086, 100002936933316, 100002946410451, 100002962685611, 100002988658758, 100002999288860, 100003015995599, 100003027130578, 100003028523477, 100003075567776, 100003075767511, 100003195537956, 100003235046757, 100003235455669, 100003236024571, 100003269432856, 100003269712266, 100003271743123, 100003286885305, 100003297152082, 100003303517895, 100003307537495, 100003321503333, 100003324408982, 100003341422735, 100003345247052, 100003370110754, 100003397217341, 100003439974922, 100003471888908, 100003487133495, 100003490700519, 100003494956120, 100003497778975, 100003497925977, 100003502009604, 100003530773801, 100003575141904, 100003586293302, 100003613474942, 100003716802577, 100003738879773, 100003767245286, 100003768605041, 100003775904470, 100003789832537, 100004205534490, 100003124538631, 100003824506450, 1591770448, 100002430485337, 100004693391269, 100005079756098,

100005038686699,100004641363150, 100004658913992,
100004675623916, 100004655852994,100004677992623,
100004630269826, 100005027312290,
100004923280127,100004880772258, 100004843601289,
100004791133905, 100004893303852, 100004842694281,
100005264921660, 100005515600057, 100005500269715,
100005626831374, 100005929773217, 100005874313876,
100006057340116, 100006077443086, 100006125011636,
100006126042473, 100006210423334, 100006249696841,
100006267764397, 100001703244792, 100001328318239.

Name: Kody Maxson, Alice Mcalister, Nicky Micky, Luth Clan, IWill SendIt,
Tiger Meow, Jennifer Plain, Miranda Todd, Michael Taylor,
Marc Burrows, Ashley Canter, Kelsey Melsey, Mel Raine, Marc Camille
Marc Camerons, Monica Stewart, Marc Camerons, Darren Miles
Marc Camerons, Kelsey Bammerz, Marc Camerons, Tyler Boo
Mary Walsh, Mary Newfound, Tyler Higgins, Shae Nora, Justin Platt,
Marc Cohen, Karoline Silverberg, Jenny Cohen, Jessica Collins,
Marc Ceefor, Mariska Cohen, Sydney Ling, Tyler Collinz
Justin Welsh, Gaby Tedford, Marc Camerons, Tyler Clinton
Mary Clifford, Cody Denisson, Jordan Stolar, Cody Cena
Olive Kubi, Marc Maceron, Cody Hoodlum, Leanna Frye
Pena Arianna, Dariana Ariana Pena Patterson, Becca Gill
Marc Camerons, Marc Camerons, Katie Fry, Tundra Manson
Kaitlin Frye, Martin Canton, Lars Merckin, Kyle Hymen Norito
Marc Camerons, Dylan Polo, Austin Collins, Marc Camer
Tomas Coco Pops (formerly Tomas Coll and Tomass Norris)
Sietse Goossens, Sidnuh Merclans, Kelseeh Rayn, Jaydeh Germanuh

MB
10/10/2013

Brandns Fathr, Brandoons Fathr, Brandon Tay, Brandons Fahtr
Bekkaah Fther, Brandons Fahter, Duckami Mahckie,
Mackieronni Gemmaro, Davee Sucret, Gemmaduck Mackieearphones
Hannuah Blaize Moar, Jehnafur Truhn, Jehenufer Trinuh
Calimestor Lempollam, Tedyuhak Matkela, Tedueye Kamalery
Tsirhc Jesus, Derrick Fischer, Marcelinda McTomas, Linda Aylin
Mirahal Cannister, Mirandela Sintaford, Merandila Simtaferd
Mintali Simtom, Terliyam Hefter, Malinday Forsent
Micantora SendingyourVideo Tombalso, Kikarino Maldonero

MS
10/10/2013

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Facebook is required to disclose the following information to the government for the user IDs listed in Attachment A:

- (a) All Machine Cookies meaning, every user that logged into his or her account from the same machine as to the Target.
- (b) Information added to the “about” section of the timeline, including but not limited to relationships, work, education, where they live and more. Any updates or changes made in the past and what is currently in the about section of the timeline.
- (c) Account Status History: dates when the account was reactivated, deactivated disabled or deleted.
- (d) Active Sessions: All stored active sessions, including date, time, device, IP address, and machine cookie and browser information.
- (e) Ads Clicked: Dates, times and titles of ads clicked.
- (f) Address: Current address or any past addresses on the account.
- (g) Ad Topics: A list of topics that may be targeted against based on the stated likes, interests and other data inputted in the timeline.
- (h) Alternate Name: Any alternate names that may appear on the account.
- (i) Apps: All of the apps that have been added.
- (j) Birthday Visibility: How the birthday appears on the timeline.

12/10/10

- (k) Chat: A history of the conversations user's had on Facebook Chat
- (l) Check-ins: The places user has checked into.
- (m) Connections: The people who have liked the users Page or Place, RSVP'd to the user's events, installed the user's app or checked in to the user advertised place within 24 hours of viewing or clicking on an ad or Sponsored Story.
- (n) Credit Cards: Any information of any purchases made on Facebook that have given Facebook credit card number information.
- (o) Currency: The preferred currency on Facebook, if Facebook Payments were utilized.
- (p) Current City: The city the user added to the about section of their timeline.
- (q) Date of Birth: The date the user added to Birthday in the about section of their timeline.
- (r) Deleted Friends: People the user has removed as friends.
- (s) Education: Any information added to the Education field in the about section of the timeline.
- (t) Emails: Email addresses added to the users account (even those they may have removed).
- (u) Events: Events user has joined or been invited to.
- (v) Facial Recognition Data: A unique number based on a comparison of the photos that the user is tagged in.
- (w) Family: Friends the user has indicated are family members.
- (x) Favorite Quotes: Information that was added to the Favorite Quotes section of the about section of the timeline.

DBS
10/10/2013

- (y) Followers: The list of people who follow the user.
- (z) Following: The list of people who the user follows.
- (aa) Friend Requests: Any Pending sent and received friend requests.
- (bb) Friends: A list of all the friends.
- (cc) Gender: The gender the user added to the about section of his timeline.
- (dd) Groups: A list of groups the user belongs to on Facebook.
- (ee) Hidden from News Feed: Any friends, apps or pages that are hidden from the user News Feed.
- (ff) Hometown: The place the user added to hometown in the about section of his timeline.
- (gg) IP Addresses: A list of IP addresses where the user has logged into their Facebook account (won't include all historical IP addresses as they are deleted according to a retention schedule).
- (hh) Last Location: The last location associated with an update.
- (ii) Likes on Others' Posts: Posts, photos or other content the user has liked.
- (jj) Likes on Your Posts from others: Likes on the user own posts, photos or other content.
- (kk) Likes on Other Sites: Likes the user has made on sites off of Facebook.
- (ll) Linked Accounts: A list of the accounts the user has linked to their Facebook account.
- (mm) Locale: The language the user has selected to use Facebook in.
- (nn) Logins: IP address, date and time associated with logins to the users Facebook account.

Handwritten signature and date:
10/10/2013

- (oo) Logouts: IP address, date and time associated with logouts from the user Facebook account.
- (pp) Messages: Messages the user sent and received on Facebook.
- (qq) Name: The name the user has on his Facebook account.
- (rr) Name Changes: Any changes the user made to the original name that was used when they signed up for Facebook.
- (ss) Networks: Networks (affiliations with schools or workplaces) that the user you belongs to on Facebook.
- (tt) Notes: Any notes the user has written and published to their account.
- (uu) Notification Settings: A list of all the user notification preferences and whether they have email and text enabled or disabled for each.
- (vv) Pages You Admin: A list of pages the user admin.
- (ww) Pending Friend Requests: Pending sent and received friend requests.
- (xx) Phone Numbers: Mobile phone numbers the user added to the account, including verified mobile numbers they have added for security purposes.
- (yy) Photos: Photos the user has uploaded to the account.
- (zz) Photos Metadata: Any metadata that is transmitted with the user's uploaded photos.
- (aaa) Physical Tokens: Badges the user has added to your account.
- (bbb) Pokes: A list of who's poked the user and who has the user poked.
- (ccc) Political Views: Any information added to Political Views in the about section of timeline.

Handwritten signature
10/25/2013

- (ddd) Posts by Users: Anything the user posted to their own timeline, like photos, videos and status updates.
- (eee) Posts by Others: Anything posted to the user's timeline by someone else, like wall posts or links shared on the user's timeline by friends.
- (fff) Posts to Others: Anything the user posted to someone else's timeline, like photos, videos and status updates.
- (ggg) Privacy Settings: The user's current privacy settings.
- (hhh) Recent Activities: Actions the user has taken and interactions the user recently had.
- (iii) Registration Date: The date the user joined Facebook.
- (jjj) Religious Views: The current information the user added to Religious Views in the about section of the timeline.
- (kkk) Removed Friends: People the user removed as friends.
- (lll) Screen Names: The screen names the user added to the account, and the service they're associated with.
- (mmm) Searches: Searches the user made on Facebook.
- (nnn) Shares Content: Anything the user shared with others on Facebook using the Share button or link.
- (ooo) Spoken Languages: The languages the user added to Spoken Languages in the about section of the timeline.
- (ppp) Status Updates: Any status updates the user has posted.
- (qqq) Work: Any current information the user added to Work in the about section of the timeline.

1/8/13
10/10/2013

(rrr) Vanity URL: The user Facebook URL

(sss) Videos: Videos the user has posted on the timeline.

II. Information to be seized by the government

All information described above in Section I that constitute fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) and (e), 2422(b), 2252A(a)(1) and (2) and (b), and 875(d) involving all the Facebook IDs identified in Attachment A.

III. By Order of the Court

1. Pursuant to 18 U.S.C. § 2705(b), the Court orders Facebook not to notify any person of the existence of this warrant until further order of the Court.

2. The Court further orders Facebook to continue to maintain the Facebook accounts associated with all the Facebook user IDs identified in Attachment A , in an open and active status so as not to disrupt this ongoing investigation.

RSB
10/10/2013